Orientering af ministeren om mulig implementering af ansigtsgenkendelses-teknologi i nattelivet

Problemstillingen

Justitsministeren ønsker at undersøge muligheden for at pålægge private virksomheder at indføre automatisk ansigtsgenkendelsesteknologi i nattelivet for at hjælpe politiets håndhævelse af reglerne. Det skal således bedømmes, hvorvidt indsamling, træning, brug og opbevaring af data i forbindelse med ansigtsgenkendelsesteknologi er lovligt. Derudover bedømmes det, hvordan privates håndhævelse af straffelovgivningen skal behandles samt, hvorvidt der kan være erstatningsansvar ved en eventuel fejlagtig udelukkelse fra nattelivet.

Baggrund

Med indførelsen af straffelovens § 79 c i 2021 er det blevet muligt at etablere opholdsforbud for personer, der er blevet dømt for voldeligt overfald, trusler, hærværk eller besiddelse af kniv i nattelivet. Opholdsforbuddet medfører, at den pågældende person ikke må færdes eller opholde sig i nattelivet i nogle specifikke nattelivszoner. På baggrund af straffelovens § 79 c er der kommet et politisk ønske om at sætte kameraer med ansigtsgenkendelses op i barer, klubber, diskoteker og koncertsteder til det formål at opdage og anholde de dømte personer, der overtræder sit opholdsforbud.

Det bør overordnet bemærkes, at det er en forudsætning for at anvendelsen af ansigtsgenkendelsesteknologi i nattelivet er i overensstemmelse med relevant lovgivning, at den bliver vedtaget ved lov i Folketinget.

I et databeskyttelsesretligt lys bør ministeren være opmærksom på en potentiel konflikt med databeskyttelseslovens § 8 i forhold til privates muligheder for at behandle personoplysninger om strafbare forhold. Muligheden for at de private virksomheder kan opbevare oplysninger om strafbare forhold efter § 8, stk. 3 – i dette tilfælde kendskabet til personer med opholdsforbud – er meget snæver og kan formentlig ikke godtages, hvis oplysningerne opbevares, så længe personen har et opholdsforbud. Jo kortere opbevaringstid, desto mindre sandsynligt er det, at opbevaringen strider imod databeskyttelseslovens § 8. Dette var tilfældet i sagen om Brøndby Stadion, hvor Datatilsynet godkendte anvendelse af automatisk ansigtsgenkendelse, da personoplysningerne blev opbevaret i så kort tid som muligt, henholdsvis få sekunder, eller hvis algoritmen fandt et match, indtil afslutningen på fodboldkampen.

Ministeren bør være opmærksom på, at ansigtsgenkendelsens fejlmargin kan være problematisk i forhold til legalitetsprincippet.

Ministeren bør også være opmærksom på, at algoritmen kan være lært på usaglige data, som giver usaglige vurderinger, hvilket kan være problematisk for saglighedsprincippet

Den menneskeretlige regulering i henholdsvis konventioner og Grundloven er ikke umiddelbart en hindring for implementeringen af ansigtsgenkendelsesteknologi i nattelivet, så længe der er den fornødne lovhjemmel, et legitimt formål og proportionalitet. I den forbindelse bør ministeren være særlig opmærksom på, at en anholdelse ikke bør ske alene på baggrund af algoritmens resultat, da algoritmens naturlige fejlmargin kan betyde, at anholdelsen ikke er proportionel.

Løsningsforslag og indstilling

Der indstilles til, at ansigtsgenkendelsesteknologi i nattelivet lovligt kan indføres, så længe visse retsgarantier er overholdt.

Ansigtsgenkendelsen bør bl.a. ikke lagre biometriske data om personer, som ikke har et opholdsforbud. Disse oplysninger bør automatisk slettes, så snart algoritmen har konkluderet, at vedkommende ikke har opholdsforbud.

For at overholde databeskyttelseslovens § 8 bør det specificeres i lovforslaget, at de private virksomheder kun får kendskab til oplysninger om personer med opholdsforbud i det tilfælde, hvor ansigtsgenkendelsen finder et match. Endvidere bør oplysningen om personen med opholdsforbud kun opbevares så længe det er nødvendigt for politiet til at håndtere sagen.

Lovforslaget bør på baggrund af legalitetsprincippet indeholde en lovfastsat accepteret fejlmargin for algoritmen, da manglende lovfastsat fejlmargin er retssikkerhedsmæssigt betænkeligt.

Saglighedsprincippet bør ligeledes fraviges ved lov, da algoritmen potentielt vil anvende usaglige data, hvorfor der vil være mulighed for, at algoritmen udfører sine vurderinger på baggrund af usaglige logikker og mønstre.

For at overholde de menneskeretlige konventioner, bør en eventuel anholdelse af en person, der er blevet matchet gennem ansigtsgenkendelse, suppleres med yderligere identifikation af politiet for at mindske vilkårligheden i anholdelser og dermed leve op til de fornødne retsgarantier og relevant lovgivning.

Bilag

1. Databeskyttelsesretlige og dataetiske problemstillinger

Det må forstås, at politiet behandler personoplysninger i form af biometriske data (ansigtsgenkendelse), når de indsamler oplysninger fra private virksomheder, som har registreret biometriske data om personer med opholdsforbud i nattelivet. Politiets behandling af personoplysninger skal vurderes i henhold til retshåndhævelsesloven. Det følger af retshåndhævelseslovens § 10, stk. 1, at det er forbudt for politiet at behandle biometriske oplysninger, hvis dette sker for at identificere en fysisk person. Efter § 10, stk. 2 kan der dog gøres undtagelse til forbuddet, hvis det er strengt nødvendigt for at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger jf. § 1, stk. 1. Brugen af ansigtsgenkendelse kan således i konkrete tilfælde tillades, hvis det er strengt nødvendigt. Det taler for at være strengt nødvendigt, at politiet ikke har ressourcer til at patruljere hele nattelivet for at sikre at ca. 200 mennesker overholder deres opholdsforbud. Yderligere kan det faktum, at alene fire personer er blevet dømt for overtrædelse af straffelovens § 79 c i 2022, potentielt være udtryk for, at politiet har manglet teknologien til at gøre den fornødne indsats på området. Det kan også tale imod at være strengt nødvendigt, at det er lykkedes at dømme fire personer i 2022 for at overtræde deres opholdsforbud, da det også kan være udtryk for at den nuværende patruljering er tilstrækkeligt. Det vurderes, at politiet kan behandle personoplysninger i form af biometriske data, da undtagelsen i § 10, stk. 2 i retshåndhævelsesloven finder anvendelse på det givne forhold.

Eftersom retshåndhævelsesloven implementerer EU's retshåndhævelsesdirektiv, skal behandlingen af personoplysninger være i overensstemmelse med EU Charterets artikel 8. I forbindelse med vurderingen i henhold til retshåndhævelsesloven vurderes der ligeledes ikke at være nogle problematikker med Charterets artikel 8 ved anvendelsen af ansigtsgenkendelsesteknologi. Det bør dog pointeres, at reglerne skal være underlagt en uafhængig myndighedskontrol, jf. EU Charterets artikel 8(3).

Når private virksomheder indsamler data ved automatisk ansigtsgenkendelsesteknologi, skal disse overholde reglerne i databeskyttelsesforordningen. Det må desuden formodes, at de private

virksomheder er i besiddelse af data om personer med opholdsforbud, hvorfor behandlingen af disse oplysninger også skal vurderes i henhold til databeskyttelseslovens § 8 om behandling af oplysninger om strafbare forhold.

Behandling af biometriske data er følsomme oplysninger og er derfor omfattet af databeskyttelsesforordningens artikel 9, stk. 1, hvorefter udgangspunktet er, at disse oplysninger ikke behandles medmindre en af undtagelserne i stk. 2 finder anvendelse. I medfør af forordningens artikel 9, stk. 2, litra g, gælder forbuddet mod behandling af følsomme oplysninger ikke, såfremt behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser. Det taler for at være en væsentlig samfundsinteresse, at man ved at benytte ansigtsgenkendelsesteknologi i højere grad kan forhindre voldelig kriminalitet og begrænse overtrædelser af opholdsforbuddet. Til støtte for dette argument, kan der drages en parallel til Brøndby Stadions implementering af automatisk ansigtsgenkendelse, som netop scannede og sammenlignede biometriske data fra de personer, der gik ind på stadionet med en intern liste over personer, som var i karantæne. Datatilsynet godkendte denne ordning i maj 2019 på baggrund af undtagelsen i databeskyttelsesforordningens artikel 9, stk. 2, litra g. Det vurderes derfor, at der i dette tilfælde også er tale om en væsentlig samfundsinteresse.

Behandlingen skal stå i rimeligt forhold til målet, der forfølges. Hertil kan eksemplet med Brøndby stadion igen fremhæves. Datatilsynet godkendte brugen af ansigtsgenkendelse med en forudsætning om, at de biometriske data om personerne, som ikke resulterede i et match med listen over personer på Brøndby IF's interne karantæneliste, ikke blev opbevaret i mere end få sekunder, mens oplysningerne om dem, som resulterer i et match, blev slettet efter kampen. Tilsvarende ved denne ordning med ansigtsgenkendelsesteknologi bør der kun lagres biometriske data om de relevante personer og kun så længe, det er nødvendigt for, at politiet kan håndhæve overtrædelsen af opholdsforbuddet. Denne begrænsning vil også sikre en overholdelse af dataetiske principper, herunder at den mindst indgribende løsning for borgerne bør vælges. Hvis dataene ikke opbevares, vil ansigtsgenkendelsesteknologien leve op til kravene i databeskyttelsesforordningen og de dataetiske overvejelser i den forbindelse.

Man bør være opmærksom på, at det tydeligt skal oplyses, at der behandles biometriske data ved brug af et automatisk ansigtsgenkendelsessystem. Endvidere skal det sikres, at personoplysninger, der opbevares, behandles på en sikkerhedsmæssig forsvarlig måde jf. databeskyttelsesforordningens artikel 32.

Da det formodes, at de private virksomheder har kendskab til de personer med opholdsforbud og dermed følsomme oplysninger i form af strafbare forhold, skal opbevaringen af disse oplysninger være i overensstemmelse med databeskyttelseslovens § 8. Det følger af bestemmelsens stk. 3, at private kan behandle oplysninger om strafbare forhold, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede. Der er en meget snæver ramme for privates behandling af strafbare forhold uden samtykke, og bestemmelsen relaterer sig mest til oplysninger, som bruges til en politianmeldelse. Hvis de private virksomheder opbevarer og har adgang til personoplysninger om strafbare forhold om personer med opholdstilladelse, vil dette potentielt være i strid med databeskyttelseslovens § 8. Det anbefales således, at de private virksomheder kun får oplysninger om personer med opholdsforbud, hvis ansigtsgenkendelsesteknologien finder et positivt match med vedkommende, således at den private virksomhed kan sikre, at opholdsforbuddet overholdes. Oplysningen bør ikke opbevares længere end nødvendigt, og dermed indtil politiet kan ankomme på stedet og overtage sagen. Ved at opbevare oplysningerne i så kort tid som muligt vil dette stemme bedre overens med den relevante lovgivning og dataetiske principper.

TV-overvågningsloven er ikke problematisk med hensyn til ved lov at indføre ansigtsgenkendelsesteknologi i nattelivet.

AI forordningens artikel 5 berører mulighederne for at anvende ansigtsgenkendelsesteknologi i retshåndhævelse øjemed. Denne bestemmelse er dog ikke relevant, eftersom dens nuværende udformning er omfattet af Danmarks retsforbehold.

Ministeren kan også gøre sig overvejelser af mere dataetisk karakter, herunder hvilket samfund ministeren ønsker, at Danmark skal være. Det kan overvejes, hvorvidt det mest centrale er at beskytte individer og bekæmpe al kriminalitet gennem overvågning, som kan være ukomfortabel og potentielt betyde, at borgere ikke ønsker at befinde sig på de pågældende steder, eller er individets ret til ikke at blive overvåget mere tungtvejende.

2. Privatlivsbeskyttelse og beskyttelse af forsamlingsfriheden

Behandling af biometriske data er som nævnt personfølsomme oplysninger og ansigtsgenkendelse er en særlig intensiv og indgribende metode, der medfører indgreb i retten til privatliv og potentielt forsamlingsfriheden.

Retten til privatliv er beskyttet i artikel 8 i Den Europæiske Menneskerettighedskonvention (EMRK), artikel 7 i EU's Charter om Grundlæggende Rettigheder, artikel 17 i FN's Konvention om Borgerlige og Politiske Rettigheder samt Grundlovens § 72. Beskyttelse af rettigheden er dog relativ, hvorfor der kan foretages indgreb i retten til privatliv, hvis der er 1) lovhjemmel, 2) indgrebet har et legitimt formål, og 3) indgrebet i øvrigt er proportionalt.

Det er centralt, at politiet sikrer lovhjemmel for at kunne benytte ansigtsgenkendelse, jf. ovenfor.

Proportionalitetsvurderingen indebærer, at der skal findes en rimelig balance mellem hensynet til individets rettigheder og hensynet til samfundets interesser eller andres rettigheder. I dette tilfælde er der et ønske at benytte ansigtsgenkendelsesteknologi til at forhindre voldelig kriminalitet samt begrænse fremtidig overtrædelse af opholdsforbud. I et sådant tilfælde bruges teknologien til et anerkendelsesværdigt formål i form af kriminalitetsbekæmpelse. Det har betydning for proportionalitetsvurderingen, hvilken form for kriminalitetsbekæmpelse, der ønskes bekæmpet. Bekæmpelse af alvorlige former for kriminalitet medfører, at der kan benyttes mere intensive indgreb. Det vil også have betydning for proportionalitetsvurderingen, om der foretages centreret overvågning af bestemte personer eller generel overvågning af borgere i det offentlige rum i form af masseovervågning. I dette tilfælde er overvågningen geografisk begrænset til barer, klubber, diskoteker og koncertsteder i Danmark i nattelivszonerne, omend disse områder også favner bredt. Derudover er det relevant, hvorvidt der er fastsat tilstrækkelige retsgarantier eksempelvis i form af rettidig sletning af data, jf. ovenfor vedrørende databeskyttelse. Det er således vigtigt, at politiet ikke blot anholder personer, når ansigtsgenkendelsesteknologien finder et match, da der kan være tale om en falsk positiv. Politiet skal således sikre identifikation på personen, før der kan ske anholdelse. Derudover skal retsgarantier i form af domstolskontrol eller anden effektiv kontrol være opfyldt og i overensstemmelse med artikel 8 i EMRK, når staten benytter overvågning.[1]

Forsamlingsfriheden er blandt andet beskyttet i EMRK's artikel 11 og Grundlovens § 79. FN's specialrapportør for forenings- og forsamlingsfrihed har udtalt, at vilkårlig overvågning af personer, der gør brug af deres forsamlingsfrihed skal forbydes. Anvendelsen af ansigtsgenkendelse kan siges at have en "chilling effect" på beslutninger om at deltage i offentlige

[1] EMD, Rotaru mod Rumænien, 4. maj 2000, præmis 57ff.

forsamlinger.[2] Det skal således vurderes, om en overvågning af nattelivszonerne udgør et indgreb i forsamlingsfriheden. Nattelivszonerne omfatter lokaliteter, der er i det offentlige rum, men der er ikke de samme beskyttelseshensyn som ved protester og politiske forsamlinger. Der er ikke tale om en generel overvågning, men rettere en overvågning rettet mod en specifik persongruppe. Under den betingelse at overvågningen ikke gemmes og lagres unødigt, vil overvågningen ikke have en chilling effect, og det vil ikke medføre et indgreb i forsamlingsfriheden.

3. Praktiske forhold om brugen af ansigtsgenkendelse

Det skal bemærkes, at diverse faktorer kan påvirke og udfordre proportionalitetsvurderingen i henhold til menneskerettighederne og hensynsafvejningerne i henhold til databeskyttelsesretten. Ansigtsgenkendelsen i den konkrete case er allerede udviklet, og kvaliteten af ansigtsgenkendelsen afhænger af algoritmen og dennes data-træning. Der eksisterer derfor en iboende risiko for, at ansigtsgenkendelsen er bias. Dette skal særligt kobles til, at ansigtsgenkendelsen tager udgangspunkt i allerede eksisterende billeddata og for at være velfungerende, skal billeddataen minde om de data, som algoritmen vil møde, når den anvendes. Endvidere vil teknologiens mulighed for korrekt identificering af personer med opholdsforbud blive påvirket af den generelle mørke belysning, blinkende lys og andre diverse faktorer såsom hudtone i den pågældende belysning, makeup og accessories, som optræder i nattelivszonerne. Dette er faktorer, som algoritmen ikke forinden vil være tilstrækkeligt forberedt på, og de vil med stor sandsynlighed medføre en større fejlmargin.

4. Forvaltningsretlige problemstillinger

Det må forstås, at man ved at kræve, at private virksomheder i nattelivszonerne opsætter videoovervågning med automatisk ansigtsgenkendelse, uddelegerer politiets faktiske forvaltningsvirksomhed til disse private virksomheder, da disse virksomheder dermed kommer til at tage del i opretholdelsen af det af domstolen pålagte opholdsforbud i nattelivszonerne jf. straffelovens § 79 c jf. Politilovens § 2, nr. 3 om politiets opgave med bl.a. at bringe strafbare forhold til ophør.

Som udgangspunkt kræver det ingen lovhjemmel at lave ekstern uddelegering af faktisk forvaltningsvirksomhed til private. Dog er der en række krav skabt af Folketingets Ombudsmands

[2] FN's Menneskerettighedsråd, "Rights to freedom of peaceful assembly and of association - Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", 17. maj 2019, A/HRC/41/41, punk 56.

praksis, som der skal overholdes, bl.a. skal offentligretlige regler og grundsætninger overholdes af AI-systemet jf. FOB 2013-9 vedrørende delegation af forvaltningsvirksomhed til Kammeradvokaten. Derudover skal de forvaltningsretlige principper om legalitet og saglighed også overholdes.

Inddragelse af legalitetsprincippet er særligt relevant i forhold til indførelse af automatisk ansigtsgenkendelse i nattelivet, da der på nuværende tidspunkt ikke er lovhjemmel for private til permanent at opsætte kameraer på de pågældende steder i mere end 1 år jf. TV-overvågningslovens § 2, stk. 6, da denne undtagelse til TV-overvågningslovens § 1, stk. 1 er midlertidig jf. bestemmelsens ordlyd.

Det bør desuden påpeges, at eventuelle falske positive og falske negative resultater fra AI-algoritmen kan være genstand for Folketingets Ombudsmands kritik. Dette var bl.a. tilfældet i FOB 2019-17 vedrørende IT-fejl hos SKAT, som SKAT ikke selv var bekendte med. Det faktum, at selv ubekendte IT-fejl kan være genstand for kritik, taler for, at den bevidste anvendelse af AI-systemer med fejlmarginen, om end denne er minimal, kan risikere at være genstand for kritik, hvilket man bør være opmærksom på ved valg af system.

Algoritmen kan også være problematisk ift. saglighedsprincippet, specielt hvis det ikke vides hvilke data, den er blevet fodret med. Dette skyldes, at disse data potentielt kan være i strid med saglighedsprincippet. Det samme gør sig gældende for de logikker og mønstre, som algoritmen kan skabe, hvorved man bør have dette med i sine overvejelser.

Derudover er der også krav til, at der ved delegation, er den fornødne myndighedsstyring og kontrol. Hvor langt dette krav til styring og kontrol rækker er uafklaret inden for forvaltningsretten. Imidlertid kan det af Folketingets Ombudsmands praksis udledes, at der skal være kontrol med algoritmens mønstre og logikker. Dette er på baggrund af FOB 2013-9, hvor Folketingets Ombudsmand lagde vægt på, at der var blevet givet en udførlig instruks til Kammeradokaten om, hvordan forvaltningsvirksomheden skulle udøves. Det samme kan siges at gøre sig gældende for algoritmen, som ikke på baggrund af dens læring må udføre forkert forvaltningsvirksomhed. Myndighederne skal holde øje med, at algoritmen ikke bruger uhensigtsmæssige mønstre og logikker, som skaber systematiske fejlagtige vurderinger.

5. Erstatningsretlige problemstillinger

Udgangspunktet må være, at der ikke vil være erstatning for en fejlagtig udelukkelse fra nattelivet, medmindre der er tale om en betydelig diskrimination eller strafbare forhold i forbindelse med udelukkelsen. Der er således en potentiel mulighed for, at staten ifalder et erstatningsansvar, hvis algoritmen bag ansigtsgenkendelsen vurderer fejlagtigt på en sådan måde, at der lides et økonomiske tab, eller at teknologien diskriminerer i en sådan grad, at det er i strid med den relevante lovgivning på området. Denne risiko vurderes dog som værende lav.